REMARKS

Reconsideration and allowance of the subject application are respectfully requested. Upon entry of this Amendment, claims 1, 2 and 4-10 are pending in the application. Applicant respectfully submits that the pending claims define patentable subject matter.

Claims 5 and 6 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite because the Examiner asserts that these claims are unclear. By this Amendment, Applicant has amended claims 5 and 6 to improve clarity. Accordingly, the Examiner is requested to remove the § 112, second paragraph, rejection.

Claims 1-2, 4-5, and 8-10 are rejected under 35 U.S.C. § 103(a) as being unpatentable over newly cited Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866) in view of newly cited Gupta et al. (U.S. Patent No. 6389532; hereinafter "Gupta"). Claim 6 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Pfleeger in view of Gupta and McClain et al. (U.S. Patent No. 6772214; hereinafter "McClain"). Claim 7 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Pfleeger in view of Gupta and Logan et al. (U.S. Patent No. 5721827; hereinafter "Logan"). Applicant respectfully traverses the prior art rejections.

Independent claim 1 is directed to "[a] method of providing access control for user terminals connected to a private network, wherein said terminals access a computer network enabling exchange of information via a private access node to which said terminals are connected and an access server. Claim 1 further recites "temporarily storing a multimedia data stream received from said computer network and addressed to a user terminal of said user

terminals connected to said private network in response to an access request from said user terminal in order to perform filtering on said multimedia data stream, said filtering authorizing or blocking transmission of said multimedia data stream to said terminal as a function of particular criteria *specified by said private network* and applied to the multimedia data stream received at said private access node." Independent claim 10 recites similar features in apparatus form.

Thus, claims 1 and 10 require that the user terminals are connected to a private network and access a computer network (e.g., the Internet) via a private access server such that requests by the user terminals to the computer network are done via the access server. These requests are not filtered but instead the responses (i.e., multimedia data stream) from the computer network are filtered. Filtering is done according to particular criteria which are specified by the private network, independently of any possible filtering rules that could be done by the public network(s) to which the private network is linked or by the computer network provider (e.g., an ISP).[1] Applicant respectfully submits that Gupta and Pfleeger, alone or in combination, do not teach or suggest these feature of the claimed invention.

The systems Gupta and Pfleeger are not in a private network. Nor is there an intermediate server. Instead, the cited references deal with direct access from a computer to the Internet wherein the filtering means reside in the user terminal.

Pfleeger does not discuss content filtering but instead is directed to packet filtering for routing purposes (to improve the QoS). The content of the packet is not analyzed. Moreover, it is not obvious to use the routers functionality of a public network in a private network as the

[1] See specification at first paragraph of page 4.

problem is not at all the same. In public network, it is the operator or the user who defines the filtering rules, whereas in the present invention, it is the private network (i.e., the company managing the private network) which specifies the filtering rules.

In a private network (the present invention), the reasons for filtering are not at all the same than in public network (avoiding costs, unjustified materials, risks for the company etc - see on 1st page). Nor is the solution the same since the private network can be linked to several public networks (in the solution of the present invention, the rules in the PBX will be independent on those of the public networks) and the router is only linked to one public network. Further, there is no temporary storing in a public network / router (in Gupta).

In a public network, the firewall (filtering) is inside the terminal. On the other hand, in the present invention, the filtering it is not in the user terminal, but instead is centralized at a private access node according criteria specified by the private network.

Accordingly, Applicant respectfully submits that independent claims 1 and 10, as well as dependent claims 2, 4-7 and 9, should be allowable because the cited references, alone or in combination, do not teach or suggest all of the features of the claims.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Christopher R. Lipp
Registration No. 41,157

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: July 17, 2006

Attorney Docket No.: Q64734